ESTIMATION OF SYSTEM FAILURE PROBABILITY UNCERTAINTY INCLUDING MODEL SUCCESS CRITERIA

James K. Knudsen[1] and Curtis L. Smith[2]

[1] Bechtel SAIC, LLC,
Las Vegas, Nevada 89144
[2] Bechtel BWXT Idaho, LLC
Idaho Falls, Idaho 83415

ABSTRACT

Uncertainty is an important part of formal decision making. Acknowledging this point, modern probabilistic risk assessments (PRAs) typically include uncertainty on parameters of the logic models used in the assessment. What is not addressed in many PRAs is the incorporation of uncertainty specific to the logic models themselves. Our paper investigates the uncertainty in the unreliability of a nuclear power plant auxiliary feedwater system. Herein, we focus on two types of uncertainty, namely "aleatory" and "epistemic." The parameter uncertainty (epistemic) for the model was determined from actual operational failure data from 1987 to 1995. Then, the system uncertainty was estimated and plotted for both aleatory and epistemic contributions. The results demonstrate that the epistemic uncertainty dominates the overall unreliability uncertainty for the auxiliary feedwater system. Factors such as the system success criteria (a type of epistemic uncertainty) can have dramatic impacts on the overall uncertainty outcome. As a result, PRA analysts may consider investing resources specifically focused on modelling uncertainty issues.

KEYWORDS

Uncertainty, epistemic, aleatory, model, parameter, PRA, risk, reliability

INTRODUCTION

Nuclear power plants are designed with many complex systems. During normal conditions, some of these systems are operating to maintain the nuclear power plant within its operating boundaries. The remainder of these systems are in standby. The standby systems are designed to operate if there is an off-normal occurrence. Because of their importance to safety, most standby systems are evaluated in the context of a probabilistic risk assessment (PRA).

The standby system that is discussed in this paper is a Westinghouse-designed auxiliary feedwater (AFW) system. As a starting point, we utilized work that was part of the "AFW system study" performed at the Idaho National Engineering and Environmental Laboratory (INEEL). (Poloski et al., 1998) This work estimated the AFW system probability of failure and the uncertainty associated with the model parameters, as is common in many PRA evaluations. (Bertucio et al., 1990) But, previous work did little to evaluate model uncertainty or uncertainty in the aleatory portions of the fault trees. In general, the evaluation of model, parameter, and aleatory uncertainty has been (largely) based on expert opinion. (Helton, 1994; Frank, 1999; Hoffman and Hammonds, 1994; Winkler, 1996)

In this paper, we will evaluate two types of uncertainty for the AFW system. The first type of uncertainty is *aleatory* uncertainty. Other names for aleatory uncertainty are “random uncertainties” and “stochastic uncertainties.” Aleatory uncertainty deals with the randomness (or predictability) of an event. For example, one may model the failure of a pump to operate, where the occurrence of failure can occur at a random time. What cannot be predicted is exactly when the pump will fail, even if a large quantity of failure data is taken.

The second type of uncertainty is *epistemic* uncertainty. Epistemic uncertainty deals with our state-of-knowledge about portions of our model. This uncertainty has been called “subjective uncertainty,” "parameter uncertainty," or “state-of-knowledge uncertainty.” Epistemic uncertainty can be viewed (and is in this report) to include both parameter-specific uncertainty and model-specific uncertainty, which are simply different levels embodied within the AFW model. The model represents a higher level than the basic events, which themselves contain another lower level, namely the parameters such as the failure rate or demand failure probability.

MODELING THE AFW SYSTEM

The AFW system is a safety-related system primarily used to provide feedwater to the steam generators and maintain a heat sink whenever there is a loss of main feedwater or a loss of offsite power. The AFW system is designed as a backup to the main feedwater system, but does not have the capacity to provide sufficient flow during normal power operations. It will automatically start and provide water to the steam generators in the event that normal main feedwater is lost. The water supplied to the steam generators by the AFW system is enough to remove the decay heat that is being produced. The AFW system operates until the reactor is at the temperature and pressure for the residual heat removal system to be placed in service, which then cools the reactor down and maintains it in a safe condition.

Before the AFW system can be analyzed, its boundaries along with the uncertainties need to be defined. To help define these parts, a “model of the world” (MOW) for the AFW system is presented in Figure 1. Figure 1 lists the model types used in this analysis and illustrates how aleatory and epistemic uncertainties fit within the AFW model. The MOW should be viewed as the mathematical model that describes the physical aspects of the system being analyzed. (Apostolakis, 1995)

The major AFW segments are broken down into separate parts for this analysis. For each segment, both aleatory and epistemic uncertainties are treated. Also, the deterministic portion of the MOW is given as the fault tree logic itself. Note that Boolean logic dictates that if gate inputs are known, then the output is known (hence it is deterministic). For this paper, the AFW system has three pumps (one turbine driven and two motor driven). These pumps feed four steam generators through discharge segments. The pumps take suction from the condensate storage tank.

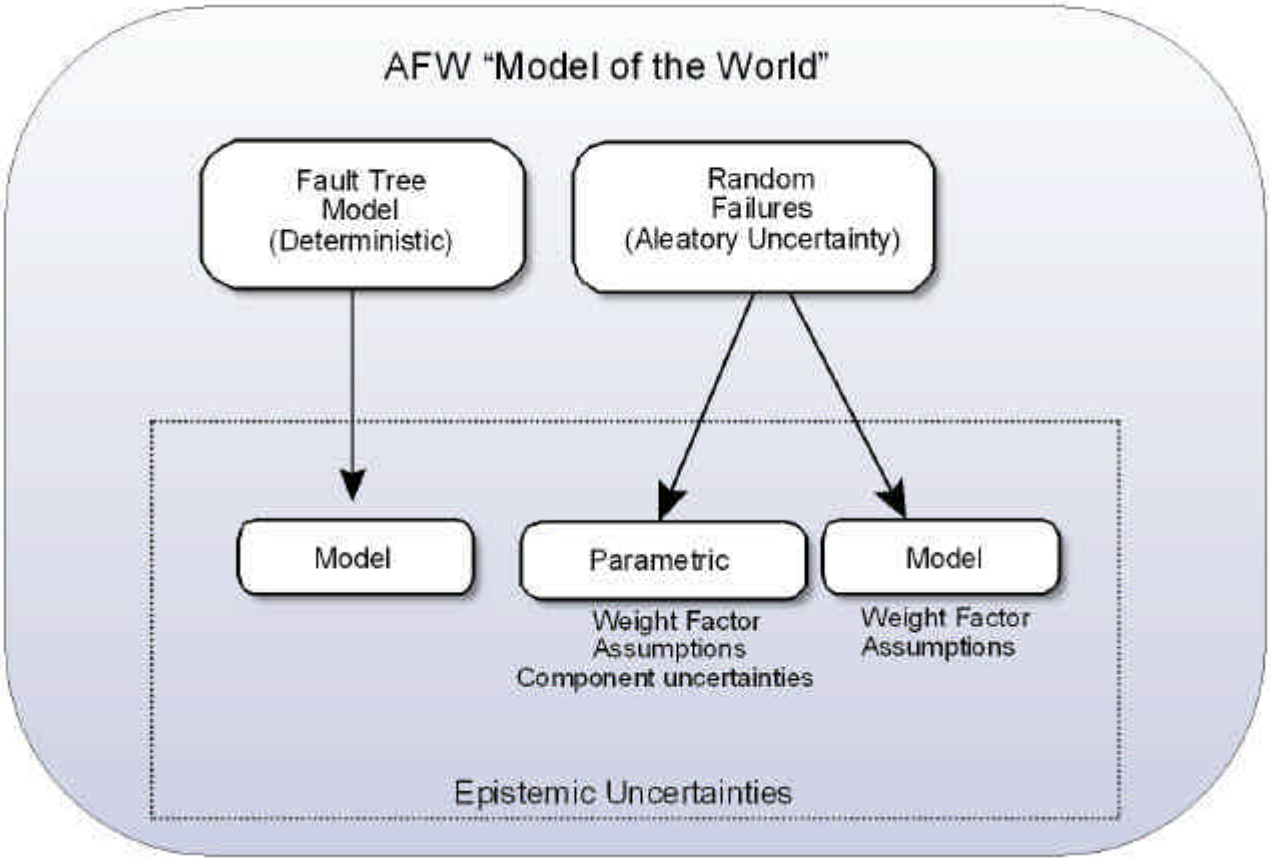

Figure 1: The model of the world structure for the example AFW system.

While the fault tree logic itself is a deterministic model, the model uncertainty is classified as epistemic uncertainty. This model uncertainty arises when assumptions are made due to our lack of precise knowledge about the system. One of the common assumptions made is that only active components are modeled. Another modeling assumption is the success criterion for the system. For the AFW system, there can be many combinations of success criteria (i.e., from one-of-three pumps feeding one-of-four steam generators to three-of-three pumps feeding four-of-four steam generators). In general, only a few success criteria are thought to be applicable, and are generally dictated by other analysis such as thermal-hydraulic evaluations (which are deterministic). A third common assumption is that partial failures are not addressed in the fault tree modeling.

The system success criteria assumption deserves additional attention. The reason for a range of success criteria stems from the types of events that can occur at a nuclear power plant. Different initiating events can require more or less AFW flow to mitigate the event. The amount of AFW steam generator cooling is generally based upon thermal-hydraulic calculations, but the parameters and boundary conditions utilized in these calculations are not known 100%. Therefore, to handle the uncertainty in the different possible success criteria, weight factors or probabilities could be assigned to each success criteria. These weight factors may then be viewed as the epistemic uncertainty of the success criteria.

With these modeling issues in mind, we are ready to develop the AFW fault tree. For this paper, the fault tree was created using the Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) program. The SAPHIRE program was developed at the INEEL. (Russell et al., 1999) SAPHIRE will use the fault tree to determine the minimal cut sets, which then dictates the unreliability for the AFW system. SAPHIRE can then be called upon to perform an uncertainty analysis.

Our AFW fault tree was constructed specifically to evaluate both aleatory and epistemic uncertainties; an example of the tree structure used is shown in Figure 2. Embedded within the AFW fault tree are weight factors tied to various success criteria; with each success criteria, the underlying Boolean logic is modified to account for the specifics of that criteria (e.g., two pumps required rather than three). Once the success criteria portion of the fault tree was developed, the individual components were modeled. Parametric (epistemic) uncertainty is accounted for via the component data, which was taken from operational experience. The AFW was modeled from the discharge section back to the suction portion of the system.

The aleatory uncertainty is accounted for by separating component-level basic events into two parts. One part represents the underlying probability model (i.e., binomial model or Poisson model) while the other part represents the "applicability" of the underling probability model. For this second part, we simply ascribed the applicability weight as either underestimating or overestimating the failure probability of the component.

The underlying probability model requires parameters such as a failure rate or demand probability. For these parameters, we assigned epistemic uncertainty based upon the data collected for the original INEEL analysis. But, because of the lack of component-specific data, the population for similar components is generally used in determining a component's failure probability. In order to better estimate an individual component failure probability (since we have a specific component, not a "population" of components), a weight factor was assigned to the component basic event.

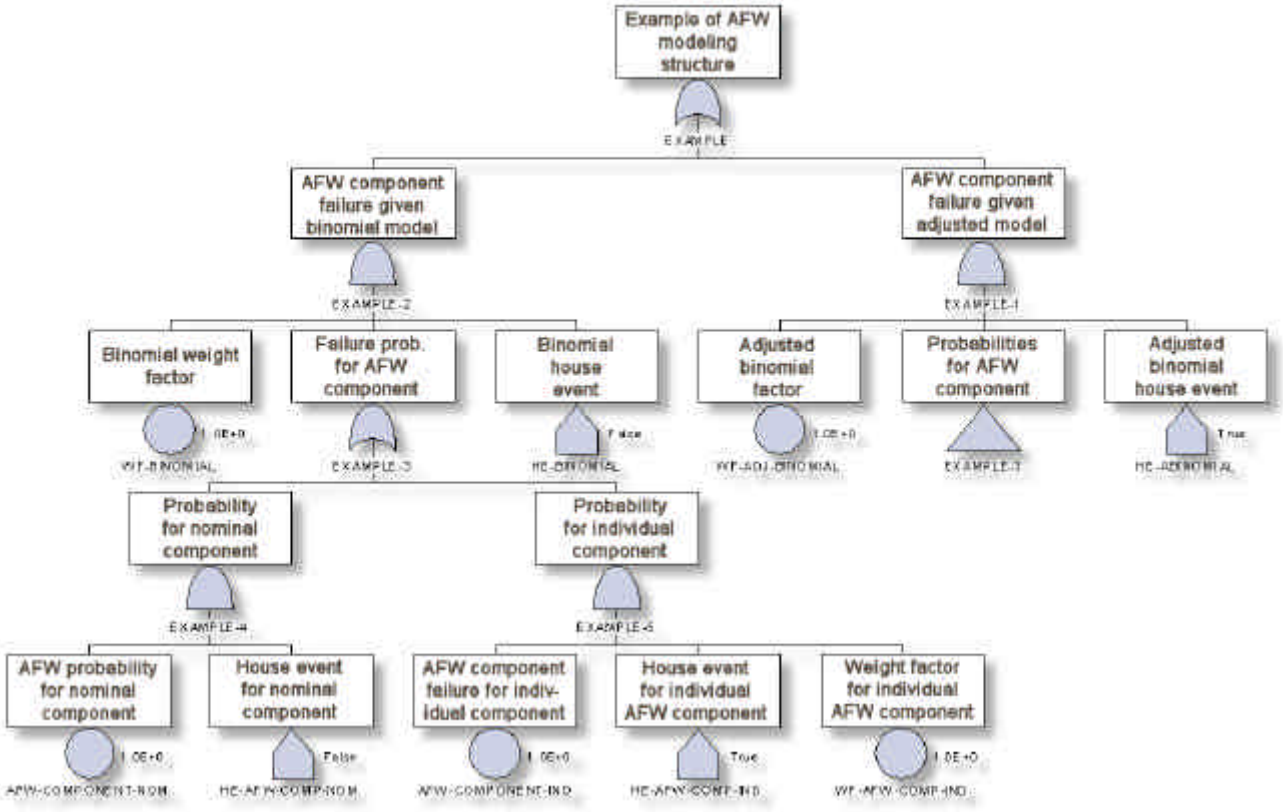

Figure 2: Example fault tree logic structure for the AFW system.

RESULTS

The AFW fault tree was analyzed to generate the minimal cut sets. Then, uncertainty analyses were performed using Monte Carlo sampling to propagate the epistemic and aleatory uncertainties through the minimal cut sets. Each uncertainty analysis run used 10,000 samples.

From each of the Monte Carlo runs, a cumulative distribution was obtained from the vector of 10,000 samples. Figure 3 illustrates the uncertainty results for two cases: (1) the model allowing just the parameter epistemic uncertainties to be sampled and (2) the model allowing just the aleatory uncertainties to be sampled. Note that the epistemic results span a much larger region than the aleatory results.

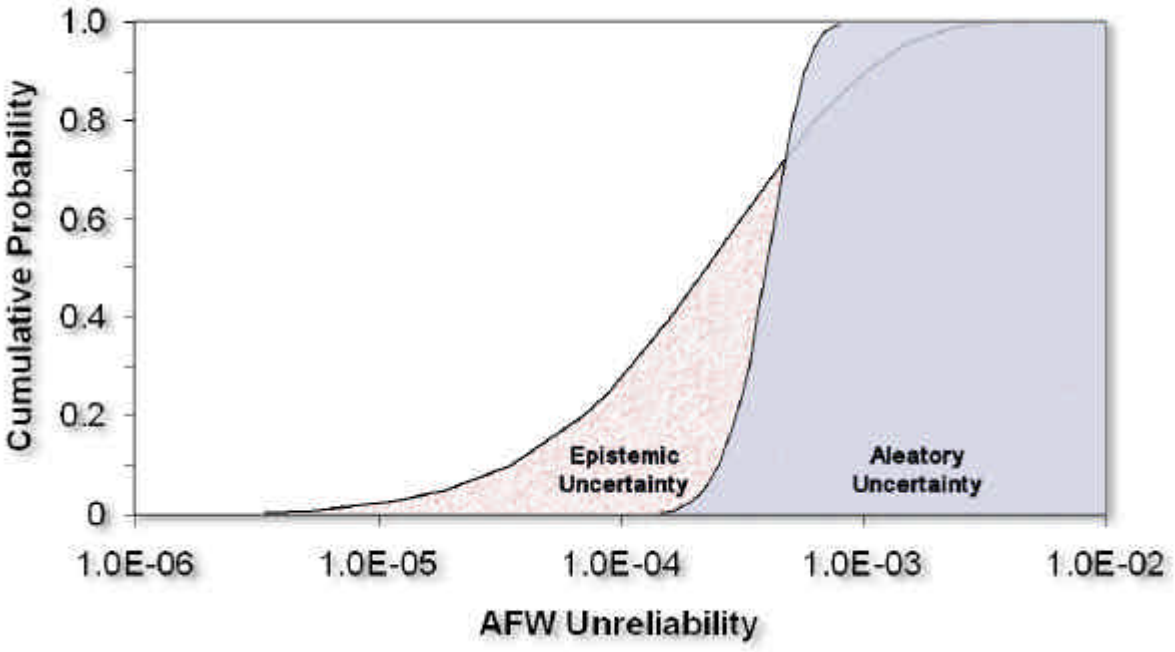

Figure 3. Uncertainty analysis results for epistemic and aleatory cases.

Now, we would like to evaluate both uncertainties in one, integrated assessment. The results from the case (1) and case (2) above, along with the combined case, are shown in Table 1. In Table 1, we list the mean and select percentiles from the uncertainty analyses. Note that the *epistemic* uncertainty portion of the combined fault tree tends to dominate the overall uncertainty results for the higher percentiles.

Table 1: Uncertainty analysis results.

		Percentiles		
Uncertainty Analysis	mean	5th	50th	95th
Epistemic (parameter) Uncertainty Analysis	4.10E-04	1.9E-05	2.2E-04	1.5E-03
Aleatory Uncertainty Analysis	4.08E-04	2.2E-04	4.0E-04	6.3E-04
Combined Epistemic and Aleatory Analysis	4.13E-04	1.7E-05	2.2E-04	1.5E–03

By modeling the fault tree with weight factors for the probability model and failure probabilities, different sensitivity analyses can be performed in order to see the effect of uncertainty. For example, we evaluated the sensitivity of the success criteria on the overall results. In this case, we assumed that the system requires 1-of-3 pumps 85% of the time (the nominal case), both motor driven pumps or the turbine driven pump 14% of the time, and all three pumps 1% of the time. We then reran the epistemic uncertainty analysis; the results of this case are shown in Figure 4. Note that even though we assumed that all three pumps will be required only 1% of the time, this assumption dominated the overall results and forced the epistemic uncertainty to be much larger than that seen in the nominal case. This behavior would indicate that analysts should be sensitive to critical modeling assumptions such as the success criteria, particularly when determining the uncertainty inherent in the model results.

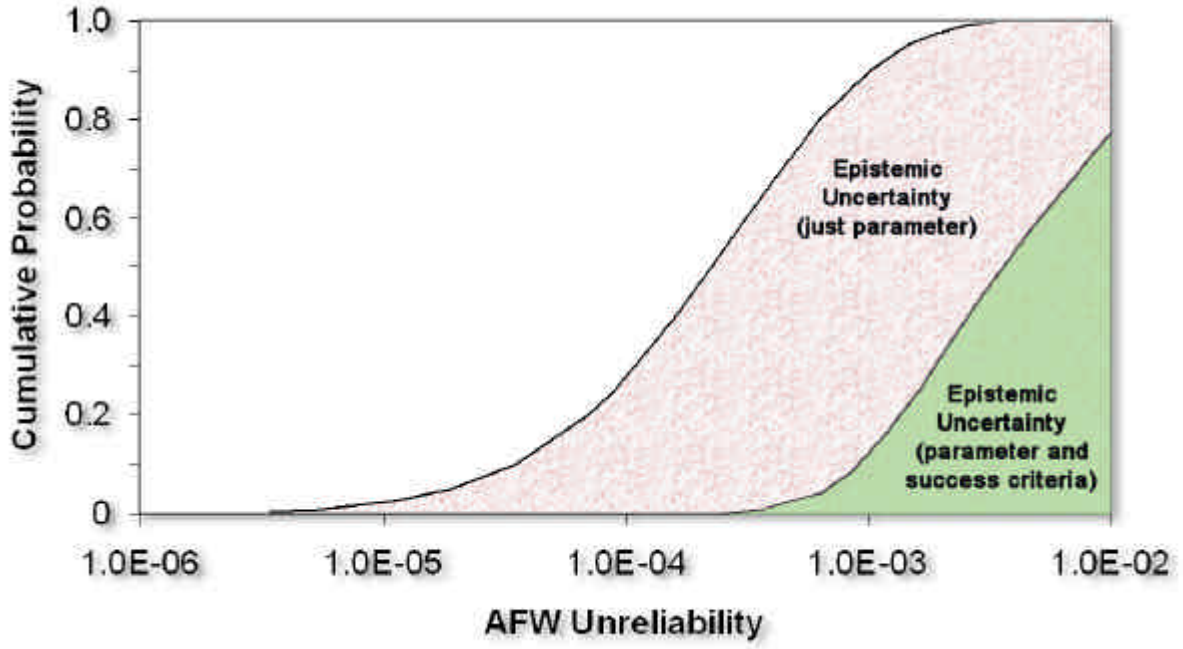

Figure 4. Epistemic uncertainty evaluations with and without success criteria variations.

REFERENCES

Apostolakis, G. E., 1995. "A Commentary on Model Uncertainty," in: *Proceedings of Workshop on Model Uncertainty,"* A. Mosleh, N. Siu, C. Smidts, and C. Lui, Eds., Center for Reliability Engineering, University of Maryland, College Park, MD (also published as Report NUREG/CP-0138, US Nuclear Regulatory Commission, Washington, DC, 1994).

Bertucio, R. C., et al., 1990. *Analysis of Core Damage Frequency: Sequoyah, Unit 1 Internal Events*, NUREG/CR-4550, Vol. 5, Rev.1.

Frank, M. V., 1999. "Assessment of the Cassini Mission Nuclear Risk with Aleatory and Epistemic Uncertainties," *Reliability Engineering & System Safety*, Vol. 66.

Helton, J. C., 1994 "Treatment of Uncertainty in Performance Assessments for Complex Systems," *Risk Analysis*, Vol. 14, No. 4.

Hoffman, F. O. and Jana S. Hammonds, 1994. "Propagation of Uncertainty in Risk Assessments: The Need to Distinguish Between Uncertainty Due to Lack of Knowledge and Uncertainty Due to Variability," *Risk Analysis*, Vol. 14, No. 5.

Poloski, J. P., et al., 1998. *Reliability Study: Auxiliary/Emergency Feedwater System, 1987 - 1995*, NUREG/CR-5500, Vol. 1.

Russell, K. D., et al., 1999. *Systems Analysis Programs for Hands-on Integrated Reliability Evaluations (SAPHIRE) Version 6.0 System Overview Manual*, NUREG/CR-6532.

Winkler, R. L., 1996. "Uncertainty in Probabilistic Risk Assessment," *Reliability Engineering and System Safety*, Vol. 54.